Veritas eDiscovery Platform™

Upgrade Overview

9.0

VERITAS

Veritas eDiscovery Platform™: *Upgrade Overview*

Last updated: 2017-11-12

Legal Notice

Veritas Technologies LLC
500 East Middlefield Road
Mountain View, CA 94043
http://www.veritas.com

VERITAS

Contents

Purpose

This document is meant to be used in conjunction with the *Veritas eDiscovery Platform Upgrade Guide*. It contains an overview to the process of upgrading and setting up the Veritas eDiscovery Platform application.

This document gives upgrade prerequisites, a process overview, and upgrade considerations for changes in the current release that involve existing data and users. This information is provided back to the last fully supported version of the eDiscovery platform.

If you are installing the Veritas eDiscovery Platform application on a machine for the first time, please read and follow the instructions outlined in the *Veritas eDiscovery Platform Installation Guide* instead of the *Upgrade* documents.

Upgrade Prerequisites

The following items need to be reviewed and addressed prior to upgrading to 9.0.

Current Version

The Veritas eDiscovery Platform 9.0 installation supports upgrades from the following versions:

- 8.1.1 GA and All Cumulative Hotfixes (CHFs)
- 8.1.1 R1
- 8.2 GA and All CHFs
- 8.3 GA and All CHFs

If you are on a previous version, upgrade to the supported upgradable version first and then upgrade to 9.0. To verify that you are at the correct product level, log on to Veritas eDiscovery Platform and select **System > Appliances**. Select the appliance and verify it is at the correct product version.

Refer to the section "*Supported Upgrade Paths*" in the *Veritas eDiscovery Platform Upgrade Guide 9.0* for details.

If using 7.1.3: Determine whether "Post April 15 2013 Purchase" Applies

Determine whether the Veritas eDiscovery Platform installation (or appliance) being upgraded was purchased after April 15, 2013. If so, refer to the Appendix for Customers Who Purchased the Veritas eDiscovery Platform After April 15, 2013 and make sure the applicable steps were followed. Contact Technical Support for assistance with fixes.

IMPORTANT! The upgrade cannot proceed if the 7.1.3 installation has not been brought into compliance with the license agreement per the instructions in the above mentioned appendix.

Web Browser Support

Internet Explorer (IE) 10 and 11 are supported end-user Web browsers.

Note: Installing and using Native Viewer requires the reviewer to be running the 32-bit version of Internet Explorer.

Note: Make sure you have the latest version of Adobe Flash Player (ActiveX Control referred to as "Shockwave Flash Object" in IE Manage Add-ons) installed in the Internet Explorer browser

to properly display the eDiscovery Platform. For Adobe Flash Player version information, see http://www.adobe.com/software/flash/about/.

Note: In version 8.3 and later, if Internet Explorer 10 users are unable to establish an https connection, make sure that the **Use TLS1.2** check box is enabled. Go to the Internet Explorer's **Tools** menu > select **Internet Options** > click the **Advanced** tab > select the "**Use TLS 1.2**" check box > click **OK**. If the appliance is running Internet Explorer 10, verify that the **Use TLS1.2** check box is enabled.

Upgrade Process Overview

Preparing for the Upgrade

The following steps need to be performed in preparation of the upgrade. Please direct any specific questions to Technical Support.

Download All 9.0 Software

Please sign in and use the MyVeritas portal for downloading product software, licensing, and support:

- Information and the replacement options are located here: www.veritas.com/docs/100040083
- For cumulative hotfix information and downloads, visit the support site Downloads area: https://www.veritas.com/content/support/en_US.html

You can download the appropriate Veritas eDiscovery Platform product files from the MyVeritas Licensing portal.

Complete Processing

In versions prior to 8.0, it was possible to upgrade to the next version of Veritas eDiscovery Platform even if processing and post processing had not completed for a case. For an upgrade to 8.1.1 or later, a case that has had its processing stopped in versions 8.1 and prior will fail to upgrade and the case will not be accessible. After upgrading, users can either re-index the case, losing all product work, or restore the case backup on the previous.
IMPORTANT! To avoid these outcomes, complete processing and post processing for all cases before performing an upgrade to version 8.1.1 or later.

Clean Up Jobs

Prior to the full node backup and upgrade, remaining eDiscovery Platform jobs should be cleaned up as appropriate on the system. This will speed up the node-backup as well as free up disk space which is important for eDiscovery Platform 9.0. You must complete all partially completed jobs before the upgrade. Refer to the section "*Cleanup Veritas eDiscovery Platform Jobs*" in the *Veritas eDiscovery Platform Upgrade Guide 9.0* for details.

IMPORTANT! Make sure to complete any unfinished jobs prior to the upgrade. After the upgrade you will not be able to retry any partially completed export jobs.

Perform a Full Node Backup

It is essential to perform a full node backup prior to the upgrade. This is a necessary operational step for all eDiscovery Platform version upgrades. Remember to stop eDiscovery Platform application services for the duration of the full node backup as well as during the upgrade.

Review Upgrade Considerations

All considerations listed in the "Upgrade Considerations" section should be fully reviewed.

Performing the Upgrade

Overview

The eDiscovery Platform upgrade should be performed by Veritas Professional Services or a certified Veritas partner.

Running Post-Processing

After the installation of the application components and eDiscovery Platform software is complete, post-processing needs to be run on all upgraded cases. As soon as the case upgrades complete, post-processing is automatically started for all cases. If necessary, the post-processing job can be stopped and restarted later if you need to change the order post-upgrade.

Licensing

Your existing license key is compatible and works with Veritas eDiscovery Platform 9.0. If you need to add additional capacity or purchase additional features, contact your Veritas Systems Engineer to request an updated license.

Note: Audio processing is a separate option and its usage is calculated differently from other PAR features. The audio processing feature requires a separate license key.

Downtime and Reboot Expectations

The Veritas eDiscovery Platform application interface will be unavailable throughout the upgrade process. The 9.0 upgrade may require one or more reboots.

Once the upgrade process completes, you will be able to login to the eDiscovery Platform.

IMPORTANT! Cases are not accessible until all case level upgrade tasks have completed. This includes case upgrade and post processing. Please refer to the table below for time estimates for these processes to complete.

The upgrade process does allow you to log in while cases are waiting for and require further update processing but this is done only to allow the System Manager to monitor the case upgrade status and to prioritize the order in which cases are upgraded. No other operations should be attempted or run.

To prioritize the upgrade order, stop any **PENDING** upgrade jobs from the **System >Jobs** page. Any cases that are already upgrading must be left to complete.

When you decide to upgrade the cases, go to the **All Processing** page and place a check mark against the case you wish to upgrade first and select the **Recover/Upgrade** button to start the job.

The time for the entire upgrade process will vary depending on number and size of the cases to be upgraded.

The following table represents general time frame expectations of key upgrade steps and may vary depending on your specific environment.

Upgrade Step	Approximate Time to Complete
9.0 Software downloads	Depends on the Internet connection and the size of the installer (for example, it might take 3-5 hours or less for

Upgrade Step	Approximate Time to Complete
	the product installer).
Full node backup	Potentially several hours depending on number and size of cases on the appliance. Typical full node backup rates are approximately 20 minutes per 1 million documents, assuming that export jobs have been cleaned up as described in the **Preparing for the Upgrade** section. Times may vary depending on the specifics of your deployment.
Veritas eDiscovery Platform application installation including upgrade of existing cases	Installation of the new eDiscovery Platform software components will take approximately 1 hour.
Case upgrade	Each case must go through a case upgrade. The time is approximately 75 minutes per 1 million documents **Note:** Please see above for how to prioritize case upgrade to ensure the most critical cases are upgraded first.
Post-processing	Typical Post-Processing rates are approximately 300,000-500,000 documents per hour. Times may vary depending on the specifics of your deployment and version of software being upgraded.

Upgrade Considerations

Upgrading from pre-9.0 to 9.0

Upgrading from pre-9.0 versions to 9.0 has the same case upgrade considerations as in "Upgrading from pre-8.3 to 8.3" in addition to the below considerations.

OST to PST Conversion Libraries

If OST conversion was previously enabled, the upgrade process automatically removes older conversion libraries (such as Datanumen) and replaces them with new OST conversion libraries. This means that if OST conversion was in use prior to the upgrade, the conversion service will continue to function but will use the newly installed library. See "New Conversion Libraries Replacing Old Ones" in technical article:
https://www.veritas.com/support/en_US/article.000128050

Upgrading from pre-8.3 to 8.3

Upgrading from pre-8.3 versions to 8.3 has the same case upgrade considerations as in "Upgrading from pre-8.2 to 8.2" in addition to the below considerations.

Additional initialization time required after a node restore

A node backup taken from a previous version must restore completely. The LDAP authentication is not available immediately after the restore because additional time is required to fully initialize. You must ensure that the node restore is complete.

Determine if the node restore is complete:

- Perform node restore: do not exit.
  Note: After the node restores completely, restart services
- Monitor the .txt file that is generated for completion of the upgrade task.
  The file is named ***esadb_<id>.txt***, where <id> is an automatically generated file number. It is located under ***<Project>/upgrade/reports/evidence_repo_<id>***.
- Locate PropertyUpgradeTask. Once the report displays "Upgrades Successful!", users will be able to login via the LDAP credentials.

For more details, see http://www.veritas.com/docs/000115951

LDAP Configuration

As of eDiscovery Platform version 8.2, the LDAP authentication passwords need to be set through the System Support Features Property Browser, as with previous releases. But ***esa.ldap.connectionPassword.enc*** is no longer entered by the users. The documentation released with 8.2 has instructions based on Clearwell Commander. However, Clearwell Commander will not be used for LDAP configuration. For instructions, see this tech note:

http://www.veritas.com/docs/000115760

Update checksum for emails

Deduplication of documents depends on matching checksums. Microsoft Office and Lotus Notes client have altered the way in which they calculate checksums. The result is that from version to version some email documents may not be deduplicated.

See also *Mandatory upgrade to Outlook 2010 and Lotus Notes 8.5 clients on Veritas eDiscovery Platform appliances and its de-dupe implications* for further background.

For example, Veritas eDiscovery Platform upgraded the version of Microsoft Office in release 8.1. For cases with previously indexed data, new emails indexed since version 8.1 may not deduplicate entirely against the emails already in the case. 8.3 provides a feature that allows a system manager (or group manager) access to the "Update Checksum for Emails" feature. This check for "Update Checksum for Emails" should be run before indexing more data.

IMPORTANT! After upgrading to 8.3, the System Manager should check to see if there is data needing the checksum update. Go to **System** > **Support Features** and choose **Update checksum for emails**. Only the cases that appear in the **Select the case** field are affected. The Case Administrator should coordinate the timing of running the "Update Checksum for Emails" feature against the affected cases.

For instructions on how to enable and use this feature, as well as feature background, case qualification criteria, workflow details, and FAQs, see http://www.veritas.com/docs/000125859.

Index Repair

The Repair Index feature solves an issue in which keyword searches were not accurate for content known to be present in the dataset for PDF, PPT, and Word files, where these files were first level attachments or loose files. Version 8.2 and later contains a fix for the issue itself, so cases created in 8.2 or later do not have the problem.

However, the ability to reindex files for a case that already had work in progress, or "reindexing in place", was required for cases set up and worked in previous versions of the eDiscovery Platform system. Once such a case is restored, the Repair Index feature allows a user with System Manager or Group Manager role to select **Repair Index** under **System** > **Support Features** for that case.

Index repair involves running a scan on each of the cases on a system. It does not need to run immediately after upgrade. Users will be able to index more data after installation, and the new data will not be affected. However, if the following two criteria apply to cases on the system, the data for these cases should be scanned as soon as is practical.

- Cases that could be affected must have been created in an eDiscovery Platform version prior to 8.2. Cases created in version 8.2 or later do not need repair.
- During the case creation Save & Setup Processing step: under "**Configure processing parameters and features**" > "**Hidden, Inserted and Embedded Content**" must have any of the check boxes selected. Case Setup default setting is "**Identify and Extract**" > "**Identify All Hidden Content**" and "**Extract all documents**". If the default values were used during case setup and there are problems with saved searches, the case is a candidate for Index Repair.

  Note: Word and PPT files affected, are from Office97 or later.

Contact the Case Administrator for cases that comply with these two points to determine whether case data should be scanned and repaired, and to coordinate timing.

IMPORTANT! See tech note 125139 at https://www.veritas.com/support for instructions, as well as feature background, case qualification criteria, workflow details, and FAQs.

Configure Browser Cache Security

Browsers, including Internet Explorer, maintain a page repository (cache) that is used to expedite the process of retrieving previously viewed pages without sending another request to the server. If a user logs out of the eDiscovery application, it is possible to press the **Back** button to view the previous page of the authenticated user. This view remains visible for just a few seconds before reverting to the login page.

A configuration setting has been added to the Security configuration which can enable or disable browser cache. If disabled, the browser cache (for example, search results) will not be stored and access or retention of sensitive information is prevented during logout. To take advantage of the browser cache security, you must uncheck the cache enabled setting. The default setting is enabled.

IMPORTANT! Once the cache is disabled, the browser will require a page refresh (F5) when the **Back** button is used to revisit certain pages (for example, navigating back through search result pages).

For those concerned about the accidental release of information possibly contained in the browser cache during the logout process, you can disable it by unchecking the checkbox for **Cache Enabled**.

- In the System view, click **Settings** > **Security**.
- Uncheck the **Cache Enabled** checkbox (checked by default).
- Click **Save**.

Restore the missing cases from case backups

In a legacy cluster, after restoring node backup on the worker node, cases on that worker node do not appear in the All Cases page. This issue occurs when the case on the restored worker node is not detected and the case does not appear in the UI.

The workaround is to individually restore the missing cases from case backups. Navigate to the **All Processing** tab > **Backups** and select a case that does not show up in the Cases list box, click **Restore** and select the target case home node and click **Restore**.

For more information, reference this article in the knowledge base:
http://www.veritas.com/docs/000122718

Adding a new worker node to DA after MySQL password is changed

When the user changes database passwords on the master and tries to update the worker node, user cannot add new worker node to DA. In this case, the user needs to do the following:

- Stop ESA services on the worker node.
- Use Password Manager to change passwords on worker to match the passwords on the master node.
- Start ESA services on the worker node.
- Restart ESA services on the worker node.
- Add the worker on the master on the Appliances screen.

For instructions, see https://www.veritas.com/support/en_US/article.000116715

Upgrading from pre-8.2 to 8.2

Upgrading from pre-8.2 versions to 8.2 has the same case upgrade considerations as in "Upgrading from pre-8.1.1 to 8.1.1" in addition to the below considerations.

Examine Access Group mappings

Starting with release 8.2, the option to select all entities such as legal hold, source, location, case, and collection set is removed in order to strengthen access group security. Therefore, users need to associate individual entities to the access group. When upgraded to 8.2 from a prior release, the system modifies the access group mappings and removes the group associations based on all entities option, and then associates individual entities with the access group. The changes in the access group mappings are reported in a new Access Group Change Report which can be accessed from the upgrade\reports folder within the product installation directory.

User Role Access Type considerations

Starting with release 8.2, you must choose Access Type when the user is created. You can assign them to an access group, or to authorize them only to specific cases. You cannot give a user both group access and case authorization. For users created in prior releases, after an upgrade to 8.2, the Case Authorized users will not be affected unless they are also associated with an Access Group. In that case, their group association will be removed. Changes that happen as a part of the upgrade process are reported in the upgrade logs.

Legal Hold authentication

Release 8.2 offers an authentication mechanism where system administrators can limit access of the legal hold confirmation page only to the intended custodians. The system administrators can choose to enable legal hold authentication so that only the intended recipients of the notice with valid LDAP accounts would be able to view and respond to the legal hold notice.

For the legal hold notices that were sent before upgrading to release 8.2, the system does not ask for LDAP authentication to respond to such notices even if the LDAP authentication is enabled after upgrading to release 8.2.

Upgrading from pre-8.1.1 to 8.1.1

Upgrading from version 7.1.5 Cumulative Hotfix 3, 7.1.5 Cumulative Hotfix 4, 8.1 Cumulative Hotfix 1, and 8.1 Cumulative Hotfix 2 to 8.1.1 has the same case upgrade considerations as in "Upgrading from 7.1.3, 7.1.4, 7.1.5, 8.0, or 8.1 to 8.1" in addition to the below considerations.

Determine the version of Enterprise Vault to use

Before performing Enterprise Vault discovery, check that the correct version of Enterprise Vault API Runtime is installed. For both new installations and upgrades from older versions, 8.1.1 automatically installs Enterprise Vault 11.0.1 API Runtime on the appliance. To connect to other certified versions of Enterprise Vault, first uninstall Enterprise Vault 11.0.1, and then re-install a certified version first. However, if you need to collect from SMTP and IMAP archives in Enterprise Vault, you must use Enterprise Vault 11.0.1.

Collect items from SMTP and Internet Mail archives

Starting with 8.1.1, when Enterprise Vault 11.0.1 is used, items from SMTP and Internet Mail archives can also be collected. When upgraded to 8.1.1, rerunning a collection task for archives with EML files will not collect the existing EML files. It can only collect new EML files that were added after the collection task was run for the last time.

Access Group permissions need to be enforced explicitly

In release 8.0, Veritas eDiscovery Platform introduced a new functionality that helps to control access to legal holds, locations, and sources. In release 8.1.1, access to collection sets can also be secured by using Access Group permissions. If you have upgraded Veritas eDiscovery Platform from an earlier release, then all legal holds, sources, locations, and collection sets are open to all users until the Access Groups permissions are enforced explicitly. Users who have collection rights to manage collection sets can enforce group access security permissions by editing the existing collection sets.

Note: Locations were introduced previously in release 8.0. Any **groups** or **locations** that were defined in 8.0 or 8.1 will remain as they were defined when they were created. However, in 8.1.1 there are changes to how **users** are affected by Group permissions that may require further administrative management.

For more information, see the Veritas eDiscovery Platform Identification and Collection Guide 8.1.1.

Upgrading from 7.1.3, 7.1.4, 7.1.5, or 8.0 to 8.1

Upgrading from 7.1.3, 7.1.4, 7.1.5, or 8.0 to 8.1 has the same case upgrade considerations as in "Upgrading from 7.1.2, 7.1.3, 7.1.4, or 7.1.5 to 8.0" and the below considerations.

Existing sources of Documentum, Livelink, and FileNet must be reconfigured to CMIS compliant sources

Release 8.1 only supports collection from Documentum 6.7, FileNet 5.1.0, and Livelink 10.5 servers with CMIS (Content Management Interoperability Services) endpoint enabled on the servers. Contact your System Administrator for enabling CMIS endpoints on your Documentum, Livelink, and FileNet servers. The non-CMIS compliant versions of these data sources are not supported. The existing sources and collections tasks/ templates created for the non-CMIS compliant data sources cannot be used as it is after upgrading to Release 8.1. To use the existing sources and collection tasks/templates, users must reconfigure their existing non-CMIS compliant sources to CMIS compliant sources. Also, if folder filter criteria were defined for the tasks/templates in previous release, then users must redefine the folder filter criteria for the existing collection tasks/templates.

Livelink E-mail collection method deprecated

The Livelink E-mail collection method is deprecated in 8.1. A new collection task or a template cannot be created with the Livelink E-mail collection method. The existing collection tasks that were created in the previous releases using the Livelink E-mail collection method cannot be re-run for collection of new or modified data. You can only re-run the existing task for custodian assignment. You can only view the task details, edit its description, create and view the defensibility report, view analytics, and create a collection set.

Configure the appliance's Outlook Profile for Office 365 and BPOS sources

Release 8.1 only supports Microsoft Office 2013. In previous release of eDiscovery Platform, the Office 365 and BPOS data sources were configured to use the appliance's Outlook Profile name as *BPOSExchangeTemplateProfile-OL2010-Do not Delete*. After you upgrade to 8.1, you must edit the Outlook Profile name to *BPOSExchangeTemplateProfile-OL2013-Do not Delete* for Office 365 and BPOS data sources.

SSL Configuration Details

By default, the SSL configuration in the eDiscovery Platform is set to accept 128-bit or greater ciphers and requires the use of TLSv1 protocol or better. SSLv2 and v3 are disabled. The set of supported ciphers and protocols can be modified if needed. Consult your IT department's security specialists to determine secure settings for your browser.

Note: If your policies require the use of TLSv1.2, certificates for all appliances must be issued by an external certificate issuing authority and installed on your servers by your own IT department. As of version 8.1, these certificates will need to be generated using a DSA authentication key.

For details on how to work with SSL backward compatibility, see Tech Note 226376:

http://www.Veritas.com/docs/TECH226376

For more information on secure LDAP SSL/TLS, refer to the *Veritas eDiscovery Platform System Administration Guide*.

Distributed Architecture Upgrade Process

Starting with 8.1, when you perform upgrade of a shared remote database server and the Cluster Master on the same machine, then you must follow the correct upgrade sequence. The database (DB) node must be upgraded first before upgrading Veritas eDiscovery Platform 8.1. Else, the upgrade process fails.

Sequence to upgrade distributed architecture:

- Stop Clearwell services on the Worker Nodes in sequence of Worker Node 1, Worker Node 2, and so on.
- Stop Clearwell services on the Cluster Master/remote DB Node.
- Run DBMS utility (*DBMSDistArchConfig.exe*) on the Cluster Master/remote DB Node.
- Install V8.1 in a new directory on Cluster Node/Remote DB Node.
- Install V8.1 in a new directory on the Worker Nodes.

  Note: Do not start the Clearwell services until you are prompted to do so once the installation is complete.
- Start Clearwell services on the Cluster Master/remote DB Node.
- Start Clearwell services on the Worker Nodes in sequence.

Uninstall Trial Versions of Microsoft Office 2010 Programs

The 8.1 installer uninstalls existing trial versions of Office 2010 Home and Business version, but NOT the trial version of Microsoft Office Professional Plus 2010. You must manually uninstall the trial version of Office Professional Plus 2010. The 8.1 installer installs trial version of Office Professional Plus 2013. You must manually activate Office 2013.

Mandatory upgrade to Outlook 2013 on Veritas eDiscovery Platform appliances and its de-dupe implications

In previous releases, Veritas eDiscovery Platform used Outlook 2010 for extracting e-mails from PSTs and MSGs. Veritas eDiscovery Platform 8.1 requires upgrade of Outlook 2010 to Outlook 2013 on Veritas eDiscovery Platform appliances as part of the 8.1 upgrade process.

During testing, we found that in some cases the email content extracted using Outlook 2013 was different than that using Outlook 2010, even though there is no documented change in the MAPI APIs and no change in the way Veritas eDiscovery Platform extracts the emails. As a result it is possible that the checksum of an email (used for identifying duplicates) can be different between the two versions of Outlook.

While this issue will not affect new cases created in 8.1, it is possible that in upgraded cases a few newly processed documents after the upgrade may not de-duplicate with the documents processed before the upgrade. In our tests, we observed 5% of e-mails that were duplicates had different checksum and thus were not identified as duplicates. With Outlook the checksums were different primarily when the e-mails were in HTML format. However, these are simply our observations. Since the behavior change is not documented by Microsoft, we do not know exactly why and when the extracted content will be different.

A warning message will be presented to the users when adding a source folder for processing new documents in an upgraded case in order to make sure they are aware of this issue.

Change in classification of items identified as “Not Imageable” in 8.0 to either “Unrecognized” or “Unsupported”

Version 8.1 can image more items than version 8.0. A few items categorized as “Not Imageable” in version 8.0 are categorized as “Unrecognized” or “Unsupported” in 8.1. If upgrading from 8.0,

items identified as “Not Imageable” during processing using version 8.0 will remain “Not Imageable”, but will be reclassified during a production or when an image cache job with “Retry previously failed documents” checked is run.

Upgrading from 7.1.2, 7.1.3, 7.1.4, or 7.1.5 to 8.0

Case restore from version 7.1.2 takes longer in version 8.x than in 7.1.5. Changes that are part of 8.x require a database table upgrade when the cases are restored. Depending on the hardware configuration and case sizes, it can take several hours for case restore to complete.

Upgrading from 7.1.2, 7.1.3, 7.1.4, or 7.1.5 to 8.0 also has the same case upgrade considerations as in “Upgrading from 7.1.3 to 7.1.4” below.

Upgrading from 7.1.4 to 7.1.5 has no case upgrade considerations.

Verify Controlled Prediction Accuracy Test Data

If you have run a Controlled Prediction Accuracy Test for a case using a previous release, then after upgrading to 8.0, you must recreate the initial and additional test sample data for the upgraded cases. For more information on the Controlled Prediction Accuracy Test, refer to the *Transparent Predictive Coding User Guide*.

Change in production behavior while producing embedded items for upgraded cases

In the 8.0 release, with the introduction of item level productions, all embedded items are automatically included as separate items within the production. While in earlier releases, there was a choice to separately produce embeddings.

When a case is upgraded from an earlier version to version 8.0, the production is not altered in anyway. However, after an upgrade to version 8.0, if a production is unlocked and then locked again, the new version 8.0 behavior is invoked. This means, if "separately produce embeddings" was not checked in the case that has been upgraded, after unlock/lock occurs in version 8.0, each embedded item will now be represented by a slipsheet in the new production.

Access Group permissions need to be enforced explicitly

Veritas eDiscovery Platform introduced a new functionality that helps to control access to legal holds, collection destinations, and sources. If you have upgraded Veritas eDiscovery Platform from an earlier release, then all legal holds, sources, and destinations are open to all users until the Access Groups permissions are enforced explicitly.
For more information, see the *Veritas eDiscovery Platform Identification and Collection Guide 8.0*.

Existing sources of DocuShare, CM8, and iManage are not available

The DocuShare, CM8, and iManage connectors have reached End of Support Life (EOSL). Starting with the release 8.0, you cannot create a new collection task or rerun an existing collection task for the DocuShare, CM8, and iManage data sources. Also, you cannot add a new source for these non-supported data sources from **All Collections** > **Sources**. The existing sources of these non-supported data sources are not shown at the Sources screen.

Upgrading from 7.1.3 to 7.1.4

Document Sent/Modified Exact Times Will Not Be Searchable for Upgraded Cases

For upgraded cases, the document will come up in Advanced Search on the date sent or last modified date, and with a time ranging from 12:00 to 11:59 for that same day. It will not be possible to select more specifically than that. For more information about using Advanced Search to find document sent/ last modified times, including email headers and LFI attributes, refer to the User Guide.

Verify Controlled Prediction Accuracy Test Data

If you have run a Controlled Prediction Accuracy Test for a case using a previous release, then after upgrading to 7.1.4, you must recreate the initial and additional test sample data for the upgraded cases. For more information on the Controlled Prediction Accuracy Test, refer to the *Transparent Predictive Coding User Guide*.

No Content Flag for Multimedia Files

For upgraded cases, the multimedia files are flagged to show the “No content found” flag and the “No indexed text” flag. New cases that are processed in 8.0 do not show these flags. The icon which indicates that no indexed text or content found for multimedia files is only displayed for pre-8.0 cases that have been upgraded. The 8.0 cases will not see this flag displayed. For more information about audio search and processing, see the *Audio Search Guide*.

Enterprise Vault (EV) Discovery must be rerun upon upgrade

When upgrading to 8.0, EV Discovery must be rerun before starting any EV-related tasks.

Tasks created in 7.1.2, 7.1.3, 7.1.4, or 7.1.5 that are in a stopped or failed state cannot be run in 8.0. Complete these tasks before upgrading. If necessary, you can copy these tasks and restart them in 8.0.

In 7.1.4, several enhancements were introduced to retry tasks in a "Partial Success" or "Partial Failure" status. The tasks created in 7.1.3 that are in a "Partial Success" or "Partial Failure" status should be copied and rerun in 8.0.

Upgrading from 7.1.2 to 7.1.3

In general, new features should work on upgraded cases unless information needs to be present at indexing time to support that new feature, or unless a new feature may have de-duplication impact.

Enterprise Vault (EV) Discovery must be rerun upon upgrade

When upgrading to 7.1.3, EV Discovery must be rerun before starting any EV-related tasks.

Tasks created prior to 7.1.2 that are in a stopped or failed state cannot be run in 7.1.3. Complete these tasks before upgrading. If necessary, you can copy these tasks and restart them in 7.1.3.

"Case Custodians" introduced to Custodian Manager will appear on Custodians page

As of version 7.1.3, Veritas eDiscovery Platform introduced a fully-integrated Custodian Management feature that allows Case Administrators to manage custodians on a case-by-case basis after that case has been processed.

Upon upgrade, custodians assigned to legal holds or collections that are assigned to cases in previous versions will also appear in the new "Case Custodians" page for upgraded cases.

Ability to Retry Failed EV Task for EV Sources will work for new collection tasks

Collection tasks against Enterprise Vault sources which result in a "Partial Success" or "Partial Failure" status can be retried, so that only the failed items are recollected. This feature only applies to new collection tasks.

EV Journal Archives Collections (Bcc and expanded DL support) will work for new collection tasks

This is the ability to collect, process, view, search, and export the fully-expanded "Bcc" and distribution list in an "envelope" format that also contains the original EV journal message. This enhancement first appeared in 7.1.2 fix pack 2.

This feature only applies to new collection tasks. On the processing and review side, the option will be disabled by default for upgraded cases created prior to 7.1.2 fix pack 2.

New Case Management dates will map to previously entered dates for upgraded cases

As of 7.1.2 Fix 2, the Case Description screen has more input options. There are now four case related date fields: **Filed**, **Served**, **Court Date**, and **Close Date**. Prior to 7.1.2 fix 2, cases had **Start Date** and **Due Date** only. Upgraded cases will have their **Start Date**s mapped to **Date Served** and **Due Date**s mapped to **Close Date**. For a full listing of the new input options, see the *Veritas Case Administration Guide*.

Improved container extraction based on strong file ID

With this feature container extraction can be excluded during discovery based on strong file ID, file extension and count. The feature is available for cases created after version 5.5, for new case folders or collection set sources added to existing cases in v. 7.1.3.

Searching using the sensitivity flag on by default; unavailable for previously created cases

For cases created on or after 7.1.3, the feature is available and on by default for newly created cases. If the user wishes to disable it, it can be done via the property browser: **esa.processing.email.sensitivity.enabled=false**

For upgraded cases in which it was previously enabled it remains enabled. For the majority of users it will not be available: it will be OFF by default for upgraded cases. It is not recommended to change the property to true if there is previously processed data, because any search will yield only partial results.

New Processing Reports – some are not supported for upgraded cases

Version 7.1.3 introduces a new UI for generating Processing reports. Of the eight options, two are not supported:

- Discovery & Processing Options is not supported for upgraded cases.
- Processing Reconciliation is not supported for upgraded cases

Also, the new **Not Processed** report will report files not processed for new cases. For upgraded cases, only not processed loose files will continue to be reported.

Directory location changed to facilitate virus scanning

Now the attachment directory path is configurable via the property "esa.altAttachmentsDir". After upgrade, users can use instructions in the System Administration guide under "**Virus Scanning Guidelines**" to configure directories using this property. For this feature to work after upgrade, the user must set the property and provide an alternative shared location with write access for the feature.

Processing properties moved from system level to case level

Cases created prior to 7.1.3 do not have case-specific crawler properties, such as for indexing, contacts, calendars, et cetera. When an **unprocessed** case created in a prior version is restored, the upgrade task will assign the system-level crawler properties to the case. Users will be able to edit the assigned crawler properties at the case level for the restored case. Note that the same assignment will occur on a node or cluster restore.

SharePoint files can be processed without depending on LFI Framework

After upgrade all new collections will be able to de-duplicate, files in containers will be processed, and internal IDs will not be exposed as Bates numbers. The same will be seen for new cases.

Improvements to search reports: impact on output

Search report exports that were previously available in .csv format are now in an .xlsx format with multiple worksheets. The keyword query filter is now item-based, so item counts will differ from the document counts shown when the filter was generated in past versions.

Lucene (third party software) upgrade task will run

An upgrade task will run to upgrade customer text indexes to match the Lucene 3.6 schema.

Family tags will propagate to items during upgrade

The propagation of family tags begins with release 7.1.3.

- Items are tagged in a manner that respects existing family-tagged document sets

- Family tags are propagated during upgrade to the items in a family (all tags in pre-v7.1.2 cases, and only non-item tags in v7.1.2 and later cases)
- Family tags can be applied from an individual item. Previously, users had to be on the parent item in review mode in order to apply a family tag. Now you can perform this action on an item and it propagates through to the entire family
- Filter counts can toggle between "document family" and "item" using the 'D' and 'I' icons
- New advanced search capabilities are available to all cases, new and legacy

Advanced Search and Tagging Scope

The new advanced search capabilities provide for a different set of scopes for the tag constraints. Some saved searches, particularly from v712, are not compatible with the new options. Should you attempt to run an incompatible saved search, an error message will display asking if you want to edit the search to conform to the expected behavior.

If you elect to edit the search, a more informative error message displays on the advanced search page detailing the problematic tagging scope choices. The incompatible tag search scopes are: "Messages and Loose Files", "Email Messages", "Attachments", "Loose Files", and "Embeddings". Searches in the "Items" scope will continue to work as expected. Most not-tagged searches are compatible. The only not-tagged scope that is *not* compatible is the situation where a user searched for "Not tagged Messages and Loose Files" in v7.1.2, and there are item-level enabled tags in the case.

Users upgrading from 7.1.2 will notice that the option previously available for Metadata/ Production Exports to propagate family tags to all items is no longer provided, since it is automatic with release 7.1.3.

For more details, see "Filtering Search Results", "Bulk Tagging Reviewable Items" and "Legacy and Current Tagging Behavior & Search Results" in the *Veritas User Guide 7.1.3*.

Email Header Search – not searchable for pre-upgrade cases

Email header data is not searchable in legacy cases. Note that the email header viewer does still work in legacy cases. Email header search is **off** by default.

Predictive Coding Graphs – Reports run before and after upgrade will appear as .csv and .xlsx

"Prediction Test" and "Controlled Prediction Test" reports that were generated in version 7.1.2 will continue to show up as .csv format files in the job pickup window and on the "Prediction Status" page after upgrade. However, newly run training cycle and test runs will generate reports in the .xlsx format with the charts in place. An upgraded case with training cycles performed before and after the upgrade will have a mixture of .csv and .xlsx reports.

Image Remediation Feature can affect caching times on some upgraded cases

In version 7.1.3 with the new image remediation feature, IGC conversion is performed on import. After an image has been successfully imported, users can review it immediately.

In upgraded cases, the "externally imaged" tag may have been applied to imported images, but in versions prior to 7.1.3 it does not guarantee completed IGC conversion. The image may still need to be converted before it can be reviewed. For cases created in a prior version, users may notice a time lag before an image can be reviewed for the first time.

Backup Area in UI Will Now Indicate if Backup Migration is Complete

For versions of Veritas eDiscovery Platform prior to 7.1.2, case backups will be migrated during upgrade to 7.1.3. If migration does not complete, a message will display with instructions.

"System" export transforms have been replaced with saved customizable versions: users may notice differences

The "system" templates (Simple DAT, Extended CSV, etc.) have been removed and re-implemented as saved, configurable templates. They can be modified, re-saved, or deleted. Although every attempt has been made to keep them as close to their corresponding system templates as possible, because there were some inconsistencies in the original system templates, minor changes such as column order may be noticed. Also, separate templates for export and production are now present for each of the system templates.

Export uses the same tool for text extraction as the indexer: users may see differences in extracted text

Because the indexer is now tracking the tool that was used for text extraction for a particular document, there is greater consistency in matching the exported extracted text to the indexed text. Users may notice some differences in extracted text between exports done in 7.1.3 when compared to the same export done in 7.1.2 and earlier.

Also, export will now flag text as having a text extraction error in audit files if "extended metadata" is selected for export and an error is encountered. This is new to 7.1.3.

OST files may be flagged during discovery as excluded

In version 7.1.3, users who bought new Veritas eDiscovery Platform licenses (or new appliances) after April 15, 2013 will encounter this. For more details, see Appendix for Customers Who Purchased the Veritas eDiscovery Platform After April 15, 2013.

For Distributed Architecture: LFI processing and post processing only supported on case home

Previously, customers were advised to use only the case home for processing LFI sources but the processing job would not fail if other nodes were provisioned for processing. In v7.1.3, the processing job will fail if any node other than case home is provisioned for processing.

New document file category: "All Images"

For upgraded cases:

- Already indexed files belonging to "All images" file category such as Encapsulated Postscript and Open Office text documents will be shown as the "Other" file category in Pre-processing Charts and Analysis & Review page. The processing report will report such files as "All images".
- Discovered sources with files in "Other" file category should be re-discovered so that files that belong to "All Images" are categorized as such and appear as "All Images" in Pre-processing Charts and Analysis & Review.

Upgrading from 7.1.1 to 7.1.2

Enterprise Vault (EV) Discovery must be rerun upon upgrade

When upgrading to 7.1.2, EV Discovery must be rerun before starting any EV-related tasks.

Tasks created prior to 7.1.2 that are in a stopped or failed state cannot be run in 7.1.2. Complete these tasks before upgrading. If necessary, you can copy these tasks and restart them in 7.1.2.

Updated Security Roles

Reduced access for Collection Admin

In previous versions, the Collection Admin role could be used for legal hold administration in addition to tasks related to collection administration. Upon upgrade, the Collections Admin role will only have privileges to view and manage collections. Existing Collection Admin users are no longer able to administer legal holds.

To grant users legal hold AND collection administration rights, you can

- Create a new role based on Legal Hold Admin rights and add collection rights as necessary.
- Assign the eDiscovery Admin role to a user to automatically grant both Legal Hold and Collections rights, among other default privileges.

New Security Role: Legal Hold Admin

The Legal Hold Admin role enables users to provide administrator-level management of legal holds. Default privileges include: access and management of legal holds; mobile access; and access to the All Cases dashboard, integrated analytics, and Case Home screen.

Legal Hold Templates Updated: Customized text must be manually reapplied

All legal hold notices are updated. Any customized legal hold templates are overwritten during upgrade.

If you customized the legal hold templates prior to upgrade, backup the templates and update the text after upgrade. These templates are accessed from **All Cases > All Legal Holds > Settings**.

New IDs are assigned to all reviewable items

Prior to 7.1.2, tags were applied to documents (also called document families). A document family is either an email with its attachments or a loose file with its embeddings. In 7.1.2, all reviewable items are assigned an item ID, and users can tag attachments and embeddings without their corresponding emails or loose files.

Saved background search results are deleted during upgrade

During upgrade, all items (emails, loose files, attachments, and embeddings) are assigned item IDs. Bitmaps with FTIDs are converted to contain item IDs. Due to these ID changes, saved background search results are deleted during upgrade.

Tag sets in upgraded cases preserve legacy behavior

By default, tag sets in upgraded cases only allow document-level tagging. Preserving this behavior enables Reviewers to continue tagging their review sets using the same logic and criteria as before the upgrade.

Tags sets that are created after upgrade have item-level tagging set by default.

To update tagging behavior, select the case. From **Case Home > Tags**, select the tag set. In the **Edit Tag Set** pane, enable the **Can be applied to individual items** option and click **Save**.

Updates to the Native Viewer requires Reviewers to install a new plug-in

An update to the native viewer requires that each Reviewer download and install a new plug-in with their internet browser. If users are not allowed to install plug-ins, an administrator needs to install the new native viewer on each system. For more information on deploying the native viewer, see the *Native Viewer (Active X) Installation Guide*.

Using imaging criteria to filter documents may create an incomplete document set in upgraded cases

In 7.1.2, users have the ability to filter documents to be cached or produced based on page count, file size, and estimated time. Because this information is calculated during indexing (a process not repeated in case upgrade), documents in an upgraded case will not have these values assigned to them. These documents could be skipped based on the file size and estimated time criteria.

In upgraded cases, do not filter documents to be cached or produced by page count, file size, or estimated time.

Slipsheet Report search filter is unavailable for locked production folders

The slipsheet report is generated when the production folder is locked. To generate this information after the case is upgraded, unlock and relock the production.

Tag names no longer case sensitive: Duplicate tags renamed upon upgrade

Prior to 7.1.2, tag names were case sensitive. Users could create a tag named "review" and a separate tag named "REVIEW". Upon upgrade, tags that rely on case sensitivity are no longer unique. These duplicate tags are renamed using the following convention: <*original tag name*>_SysRenamed<*count*>.

Note: If the length of the new tag name exceeds the character limit of 255 characters, users must rename the duplicate tag manually.

New Case Backup Folder Hierarchy

With 7.1.2, a new folder named "cases" is added to the case backup folder hierarchy. Case backups now use the following folder hierarchy: caseBackups\cases\<*caseid-casename*>.

During upgrade the new folder hierarchy is set up automatically. However, if you manually copy the case backup files into the backup folders, ensure that you use the new hierarchy.

New Folder Wizard

To access the new folder wizard, run a search query from **Analysis & Review**. Then from the **Actions menu,** select **Folder.** The wizard guides you through selecting the items you want to affect and determining whether you want to copy, move, or remove the selected items.

Previously, these tasks were performed from the **Actions > Tag** window.

Search Filters return different counts due to item-based searches

File Type search filter counts each item—not each document-family

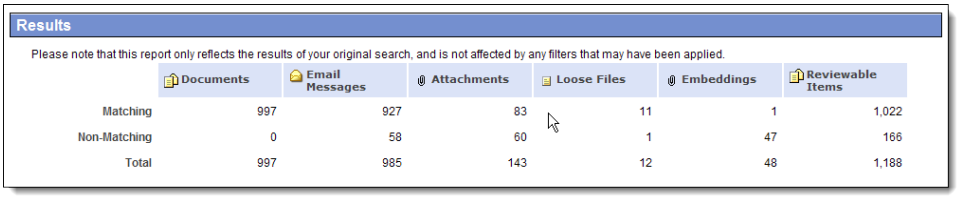
Prior to 7.1.2, the File Type search filter worked at a document-family level. If a document family (an email or loose file) contained an attachment or embedding of a specific file type it was counted once, whether there was one item of that file type or several.

Because the File Type search filter is now an item-level filter, the File Type search filter counts every item of a specific file type. If an email has 50 Microsoft Word files attached, all 50 documents are counted.

Tag search filter results might cause confusion when used with basic keyword searches in upgraded cases

The Tag search filter is now an item-based filter. Prior to 7.1.2, all tag sets were applied to a document family rather than a specific item. Because of this change, search filter result counts will be different after upgrade.

To learn more about how the search filter counts were calculated, see the Search Report.


Results

Please note that this report only reflects the results of your original search, and is not affected by any filters that may have been applied.

	Documents	Email Messages	Attachments	Loose Files	Embeddings	Reviewable Items
Matching	997	927	83	11	1	1,022
Non-Matching	0	58	60	1	47	166
Total	997	985	143	12	48	1,188

Upgrading from 6.6, 7.0, 7.1 to 7.1.1

The following items may affect cases when upgrading from 6.6, 7.0, 7.1 to 7.1.1 and should be reviewed prior to the upgrade with Technical Support

Note: To upgrade from 6.6, you must be running either Fix 3 or Fix 4 software patches.

Mandatory upgrade to Outlook 2010 and Lotus Notes 8.5 clients on Veritas eDiscovery Platform appliances and its de-dupe implications

In previous releases, Veritas eDiscovery Platform used Outlook 2003 for extracting e-mails from PSTs and MSGs, and Lotus Notes version 7.0 for extracting e-mails from NSFs. Veritas eDiscovery Platform 7.1.1 requires Outlook 2010 and Notes 8.5, requiring upgrade of these two products on Veritas eDiscovery Platform appliances as part of the 7.1.1 upgrade process.

Note: If you are upgrading from 7.0 or 7.1 to 7.1.1, then the appliance is upgraded to Outlook 2010 and Notes 8.5 as part of the 7.0 or 7.1upgrade.

During testing, we found that in some cases the email content extracted using Outlook 2010 was different than that using Outlook 2003, even though there is no documented change in the MAPI APIs and no change in the way Veritas eDiscovery Platform extracts the emails. A similar behavior has been observed between Notes 7.0 and Note 8.5. As a result it is possible that the checksum of an email (used for identifying duplicates) can be different between the two versions of Outlook and between the two versions of Lotus Notes.

While this issue will not affect new cases created in 7.1.1, it is possible that in upgraded cases a few newly processed documents after the upgrade may not de-duplicate with the documents processed before the upgrade. In our tests, we observed 10 to 15% of e-mails that were duplicates had different checksum and thus were not identified as duplicates. With Outlook the

checksums were different primarily when the e-mails were in HTML format, and with Lotus Notes the checksums were different when the e-mails had foreign language content. However, these are simply our observations. Since the behavior change is not documented by Microsoft or by IBM, we do not know exactly why and when the extracted content will be different.

A warning message will be presented to the users when adding a source folder for processing new documents in an upgraded case in order to make sure they are aware of this issue.

MBOX Email Conversion De-Dupe Implications

Due to an upgrade in Aid4Mail software, attachment handling was changed in cases where an attachment was missing or the attachment was pointing to an unresolved URL. This could result in a small percentage of MBOX emails not duplicating against previously converted emails.

Due to improved handling of EMLX content, some EMLX documents may not de-dupe with previously-processed EMLX documents

In previous releases, if the XML properties were not properly separated from the body, they were processed as the body content. Veritas eDiscovery Platform 7.1.1 properly identifies those properties even they are not properly separated from the body content. As a result, it is possible that some EMLX e-mails processed after upgrading to 7.1.1 may not de-duplicate with those processed prior to the upgrade.

Note: This change should not impact 7.0 or 7.1 upgraded cases.

Post-processing cannot be stopped once it has started.

Veritas eDiscovery Platform processes documents in two stages: indexing and post-processing. The indexing stage identifies duplicates and builds full-text index by extracting content from the documents. The post-processing stage builds analytics, like domain filters, discussion threads and concepts, and performs integrity check of the index before completion. In previous releases, user can stop the job in either of the two stages, add more documents for processing, and the system would index the newly added documents and do post-processing of both old and new documents together.

With version 7.1.1, users cannot stop post-processing jobs and add more documents for processing. Once the post-processing has started, it must complete before user can add more documents to the case. Users still have option to stop indexing and add more documents for processing before the post-processing has started.

Partially processed data cannot be searched

In previous releases, users could search partially processed data during a processing job. If data was incomplete the user would see a yellow warning message indicating the incomplete state. In Veritas eDiscovery Platform 7.1.1, data from the current processing job will not be visible until processing is complete.

Processing exception counts for cases prior to 5.0

For cases created in v5.0 or before, the counts for **Processing > Exceptions** – File Notices may not add up to the counts on Exceptions – Message Warnings. Contact Technical Support if this is an issue.

Check the disk space in your database before you start case processing

If the database runs out of disk space during case processing, increase the disk space and either restart case processing or restore the case from a backup and resume processing.

Export Features and Considerations

Partially finished export jobs from a previous version cannot be retried or finished post-upgrade.

Export batching uses document count

For Metadata and Production exports, users can now split export output based on the number of document families (for example, an email message with all of its attached files constitutes one type of document family), that it contains. Prior to 7.1.1, the export output was split based on the XML file size.

Note: The default grouping of documents is 3,000 and the maximum number is 5,000.

Improved handling of retry documents

Retried documents are inserted directly into the original export folders. Previously, retry folders were created for each retried job.

Shared location for source NSF files

When users select the option to include native files and the source includes NSF file types, the output for the NSF files is placed into a shared folder (NSFfiles) and no longer in an XML-specific native folder.

Export job changes in created XML files

Export jobs now update the existing summary XML file with total number of documents exported instead of creating new summary XML files for each job. The `output_urn.xml` file is no longer created with an export job. Starting with 7.1.1, the `input_urn.xml` lists all attempted documents rather than only retried documents.

Support of Legal Hold Activity Report for upgraded holds

All of the legal hold reports (Activity, Defensibility, and Survey reports) are the same between 7.1.1 and upgraded holds with the following exception:

- If a legal hold custodian responds multiple times to their hold (usually this is the case where the custodian decided to change a survey answer) before upgrading to 7.1.1, only the last version of their answers is retained. Any history of their prior responses will not appear in the Legal Hold Defensibility Report. If a custodian responds again after the upgrade to 7.1.1, any responses prior to the upgrade are lost.

The following items are applicable if you are upgrading directly from 6.6 to 7.1.1. If you are upgrading from 7.0 or 7.1 then these changes were already in effect in 7.0 and 7.1.

Saved Searches created using file type filters may have different results count after the upgrade

Starting with Veritas eDiscovery Platform 7.0 a few of the image types that were reported under “other types” category are now reported under “all images” category in the file type filter. As a result, saved searches created using “other types” and “all image” categories in the file type filter prior to upgrade may have different results count after the upgrade.

Topics are disabled

In previous releases, Veritas eDiscovery Platform automatically identified key topics based on the noun and noun phrases found in the documents. Starting with Veritas eDiscovery Platform 7.0, this capability is disabled. Users will not see topics for new cases as well as for the upgrade cases. For upgraded cases, the topics that were created prior to the upgrade are only visible from the Analysis & Review menu after the upgrade to 7.1.1. Note that Veritas eDiscovery Platform now includes Transparent Concept Search, a feature that provides a powerful way of locating documents and refining searches based on concepts.

Configurable export templates are replaced with global export templates

In prior releases, each user had an option to create three custom export templates – configurable template 1, configurable template 2 and configurable template 3. These templates were for personal use only and were not sharable across cases and with other users. Starting with Veritas eDiscovery Platform 7.0 users have the ability to create global export templates. Users can now share export and production templates across multiple cases and with other users. The custom templates created in the prior versions of Veritas eDiscovery Platform will not be available after the upgrade to 7.1.1.

New permissions for controlling access to tag event comments and documents notes

Starting with Veritas eDiscovery Platform 7.0, new privileges are introduced to control user's ability to view tag event comments and document notes. Users which have global roles, such as system administrators, will automatically get the permissions for both tag event comments and document notes access. Users which have case roles, such as case administrators, will get these permissions only if they have tag history search and view permissions.

The ability to filter documents by languages is not available for cases upgraded from V3.0 and V4.0

For cases upgraded from Veritas eDiscovery Platform 3.0 or 4.0 to 7.1.1, the ability to filter documents by languages will not be available for the existing case documents as well as for the newly processed documents after the upgrade.

Appendix for Customers who purchased the Veritas eDiscovery Platform after April 15, 2013

After April 15, 2013, new Veritas eDiscovery Platform customers must follow the instructions below or they will be out of compliance with their Veritas eDiscovery Platform license agreement.

Note: Existing customers do not need to follow these steps **unless** they have purchased a new appliance after April 15, 2013.

For Customers who purchased Veritas eDiscovery Platform starting with version 7.1.3

IMPORTANT! After April 15 2013, new Veritas eDiscovery Platform customers needing to perform OST to PST file conversion should obtain their own license for "Advanced Exchange Recovery", or use alternate means for file conversion.

Before using the Veritas eDiscovery Platform product, the user must consider the following options:

- In version 7.1.3, OST files will be flagged during discovery as excluded to give customers the opportunity to use alternate means to convert them to PST files for Veritas eDiscovery Platform processing.
  Note: If the user disables "Convert mail formats (OST, MBOX) to PST" in case settings, then all OST and MBOX files will be treated as loose files.
- Alternatively, the customer can covert the OST to PST format before ingesting the data.

For Customers who purchased Veritas eDiscovery Platform after April 15, 2013 and are upgrading to 7.1.3

IMPORTANT! To be in compliance with their Veritas eDiscovery Platform license agreement, new customers who purchased the Veritas eDiscovery Platform (or who have purchased a new appliance) after April 15, 2013 **must be on the following version before attempting to upgrade to 7.1.3**:

- The software installation or appliance to be upgraded **must** be on version 7.1.2 Fix2, with Hotfix ESA-30819 applied (see below for the hotfix exception). Contact Technical Support for assistance with fixes.

Before using the Veritas eDiscovery Platform product, the user must consider the following options:

- For users on version 7.1.3, OST files are flagged during discovery as excluded to give them the opportunity to use alternate means to convert them to PST files for Veritas eDiscovery Platform processing. For 7.1.2 users, OST files will error at discovery time for the same purpose.
  Note: If the user disables **Convert mail formats (OST, MBOX) to PST** in case settings, then all OST and MBOX files will be treated as loose files.
- Alternatively, the customer can covert the OST to PST format before ingesting the data.